Appendix C

Electronic Deception

Electronic Deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of EM energy in a manner intended to convey misleading information and to deny valid information to an enemy or to enemy electronic dependent weapons. Electronic deception is both parts of EW and military deceptions. Normally, an electronic deception is conducted as part of a larger deception, and are seldom conducted alone. Division is the lowest level at which a deception plan can be initiated, and the commander must approve all deception plans. Historically, deception operations originate from EAC.

TYPES OF ELECTRONIC DECEPTION

C-1. Among the types of electronic deception are—

- **Manipulative Electronic Deception (MED).** Actions to eliminate, reveal, or convey misleading, telltale indicators that may be used by hostile forces.
- **Simulative Electronic Deception (SED).** Actions to represent friendly, notional, or actual capabilities to mislead hostile forces.
- **Imitative Electronic Deception (IED)**. The introduction of EM energy into enemy systems that imitates enemy emissions.

C-2. Although electronic deception is usually thought of in terms of communications, electronic deception is also conducted using digital (analog) emissions. The signals could mimic the data flows issuing from a TOC when in reality it is a jammer putting out a signal pre-recorded for this mission.

MANIPULATIVE ELECTRONIC DECEPTION

C-3. MED uses communication or noncommunication signals to convey indicators that mislead the enemy. For example, to indicate that a unit is going to attack when it is actually going to withdraw, the unit might transmit false FS plans and requests for ammunition.

C-4. MED is used to cause the enemy to splinter his intelligence and EW efforts to the point that they lose effectiveness. It is used to cause the enemy to misdirect his EA and ES assets and therefore cause fewer problems with friendly communications. Used in these ways, MED is an EP technique.

SIMULATIVE ELECTRONIC DECEPTION

C-5. SED uses communication and noncommunication signals to mislead hostile forces as to friendly units and/or the capabilities of friendly units. There are three types of SEDs:

- **Unit Simulation.** The use of actual equipment or specially designed simulators to indicate that a unit is in a certain location during a specified period.
- **System Simulation.** The use of systems that give off emissions peculiar to a particular organization. A countermortar or counterbattery radar is peculiar to an artillery unit; therefore, by turning on that type of radar you can indicate the probable location of an artillery unit.
- **Activity Simulation.** The operation of noncommunication emitters to imply a type or change of activity by a unit. For example, placing surveillance radars in a typical defensive array when, in fact, the intention is an attack.

IMITATIVE ELECTRONIC DECEPTION

C-6. In IED, the enemy's EM emissions are imitated to mislead the enemy. Examples include entering the enemy communication nets by using his callsigns and radio procedures, and then giving enemy commanders instructions to initiate actions which are to our advantage. Targets for IED include any enemy receiver and range from cryptographic systems to very simple, plain-language tactical nets. IED can cause a unit to be in the wrong place at the right time, to place ordnance on the wrong target, or to delay attack plans. Imitative deception efforts are intended to cause decisions based on false information that appears to the enemy to have come from his own side.

C-7. Properly used, IED can be decisive on the battlefield. However, to be effective, IED requires electronic equipment capable of convincingly duplicating the functions of enemy equipment. IED is done if—

- (The transmitter) is compatible with the intended receiver station equipment.
- (The transmitter) has sufficient power to transmit to the receiver station.
- A proficient linguist (if voice transmissions are used).
- An operator capable of imitating the transmitting style of the enemy manual Morse operator (if continuous wave is used).

C-8. If available, however, captured enemy equipment (CEE) should be used to ensure that the technical characteristics of signals are authentic.

ELECTRONIC DECEPTION PLANNING

C-9. Electronic deception planning determines how to use EM equipment to mislead the enemy and cause him to do something to our advantage. Each

piece of electronic and associated equipment has its own electronic signature. These signatures are exploited in deception.

C-10. The G3 usually plans and supervises deceptions. The EWO is usually responsible to the G3 for the electronic deception plan. All of these personnel work with the G2 to determine the electronic activities most likely to be intercepted by enemy SIGINT.

C-11. Careful integration of electronic deception with visual, sonic, and olfactory actions is critical. What the enemy detects electronically must remain consistent with other sources of intelligence reports. Because of the reliance placed on EM radiation (for example, communication, surveillance, navigation) this aspect of deception requires close attention. Although electronic deception can be the sole act of deception, the effect is often of short duration.

C-12. The enemy's success depends upon his knowledge of your emitters. Success in MED and SED depends on understanding how your emitters appear to the enemy. The SIGINT team should keep a profile (database) of a command's voice and digital (analog) emitters. This is to determine how best to electronically portray a desired portion of that command. When planning MED and SED, it is usually necessary to consider all the command's EM emitters. It is necessary to consider what is occurring and what should occur with all EM emitters in the unit's area.

C-13. Similarly, when planning an electronic deception, consider all unit electronic activities, such as—

- Actions that support the current operation as well as those that will support the deception operation.
- All actions which must be integrated and deconflicted to prevent one activity interfering with another.

C-14. Some considerations for planning are—

- Close control and coordination will be necessary, especially during MED.
- The staff plans to avoid confusing friendly operators with deception communications or with unique returns on digital (analog) equipment.

C-15. Time is critical. Given sufficient time, the enemy can discover even the most complex electronic deception. A deception intended to deceive the enemy for two or three days must include a well-coordinated electronic deception that covers all electronic emitters.

- Adequate for a deception for only a short period just before an attack.
- The electronic deception plan can be relatively simple.
- Enemy capabilities are critical. If the enemy cannot detect your electronic emitters, the electronic deception will fail.

C-16. The commander can perform MED and SED as long as he uses only equipment under his control. IED can only be done with permission of the appropriate commander—within a division, this is usually the division commander. This restriction is to ensure that IED does not jeopardize the SIGINT effort. IED, if recognized by the enemy, will provide data concerning

the friendly ES effort. This could cause the enemy to improve his communications security (COMSEC) and procedures to reduce the effectiveness of the friendly SIGINT efforts. Coordination with higher will always occur before any MED or SED operations begin.

C-17. False emanations must be—

- On signals strong enough to reach the enemy.
- On a frequency the enemy can intercept.
- In a modulation the enemy can intercept.

ELECTRONIC DECEPTION TECHNIQUES

C-18. The following are electronic deception techniques:

- Leave a significant sample of regimental or battalion headquarters communication in place while the headquarters moves to another location.
- Broadcast false information with the intention of having the enemy receive the message and commit his forces into an area of our choosing.
- Broadcast false unit strengths, dispositions, or locations to confuse the enemy.
- Exchange operators among units or overload one unit with operators whose characteristics are probably known to the enemy.
- Place multichannel communications in a battalion area to show a larger force.
- Pad traffic on secure links to deceptively show a buildup for an attack. This technique applies to both voice and message traffic when encrypted.
- Use callsigns and frequencies to lead the enemy to incorrect net structures.